サイバーセキュリティタスクフォース（第 34 回）議事要旨

1. 日 時）令和 3 年 10 月 14 日（木）10：00～12：00

2. 場 所）オンライン

3. 出席者）

【構成員】

後藤座長、安達構成員、鵜飼構成員、岡村構成員、小山構成員、篠田構成員、園田構成員、戸川構成員、徳田構成員、中尾構成員、名和構成員、林構成員、藤本構成員、吉岡構成員、若江構成員

【オブザーバー】

扇慎太郎（内閣サイバーセキュリティセンター）、篠崎美津子（デジタル庁）、渡邊貴史（経済産業省）、石川家継（地方公共団体情報システム機構）

【発表者】

井上大介（情報通信研究機構（NICT）サイバーセキュリティ研究所）

【総務省】

巻口サイバーセキュリティ統括官、山内大臣官房審議官（国際技術、サイバーセキュリティ担当）、湯本サイバーセキュリティ・情報化審議官、梅村サイバーセキュリティ統括官室参事官（総括担当）、高村サイバーセキュリティ統括官室参事官（政策担当）、海野サイバーセキュリティ統括官室参事官（国際担当）、安藤サイバーセキュリティ統括官室企画官、佐々木サイバーセキュリティ統括官室統括補佐、廣瀬サイバーセキュリティ統括官室参事官補佐、須藤住民制度課デジタル基盤推進室課長補佐（代理出席）

4. 配付資料

資料 34-1　「ICT サイバーセキュリティ総合対策 2021」に基づく取組
資料 34-2　令和 4 年度総務省サイバーセキュリティ関連予算概算要求について
資料 34-3　IoT セキュリティに関連する近年の研究内容の紹介（吉岡構成員）【配布は関係者限り】

5. 議事概要

（1）開会

（2）説明

◆議題（1）「「ICT サイバーセキュリティ総合対策 2021」に基づく取組」について、事務局より資料 34-1 を説明。議題（2）「令和 4 年度総務省サイバーセキュリティ関連予算概算要求」について、事務局より資料 34-2 を説明。議題（3）「IoT セキュリティに関連する近年の研究内容の紹介」について、吉岡構成員より資料 34-3 を説明。

◆構成員の意見・コメント

【資料 34-1　「ICT サイバーセキュリティ総合対策 2021」に基づく取組について】

若江構成員）

「電気通信事業におけるサイバー攻撃への適切な対処の在り方に関する研究会」（以下、「サイバー研」という。）における検討の状況において、フロー情報で C&C サーバを検知することが正当業務行為であるという件について、私は、違法性阻却事由で整理するのではなく、むしろ立法で対応する必要があるのではないかという問題意識であり、以前のタスクフォースでもその旨発言した。その上で、今回の結論について、いくつか分からないことがあったので教えていただきたい。１点目に、ISP が取得しているフロー情報で C&C サーバを検知するということが挙がっているが、そもそもフロー情報取得の適法性というのは確認されているのか。２点目に、第三次とりまとめにおいては、役務提供に支障が生じるおそれがあるかどうか不明確な時に利用者全体を対象として行う取組については、行為の必要性・手段の相当性を肯定しがたく正当業務行為と整理するのが困難とされていたと思う。しかし第四次とりまとめ案においては、第三次とりまとめ以降のサイバー攻撃の状況が変化して予防的対応の必要性が高まっているとして、行為の必要性・手段の相当性を肯定している。予防的対応の必要性が高まってしまうとかつて否定された行為の必要性と手段の相当性が肯定されるというのがなぜなのか知りたい。特に手段の相当性の方は、対策の必要性とは別に判断されるような要件ではないかと思うので、サイバー研では刑法の専門家の方からどのような意見が挙がっているのか教えてもらいたい。３点目に、C&C サーバに関する情報の共有について、とりまとめ案の 13 ページに、C&C サーバに関する IP アドレスとポート番号をとりまとめてリスト化したもの、すなわち、個別の通信から把握されていても個々の通信の構成要素を明らかにすることにはつながらないと記載があるが、これは通信の秘密ではないという趣旨であるかどうかという確認をしたい。

名和構成員）

同じく「電気通信事業におけるサイバー攻撃への適切な対処の在り方に関する研究会」における検討の状況について、C&C サーバに関する情報の「適切な事業者団体等への提供」という説明があったが、この「適切な」の判断基準は総務省などが今後、基準を示すのか。あるいは、各 ISP が独自に判断するのか。また、サイバーセキュリティ対策の目的に限定し提供するとのことであるが、これはサイバーセキュリティ対策の製品・サービスの改善・開発に係る目的を念頭に置かれているのか。営利のために使われることを許容しているのか確認したい。

梅村サイバーセキュリティ統括官室参事官）

若江構成員からのご指摘について、今回の議論にあたっては、目的の正当性・行為の必要性と併せて手段の相当性も十分にご議論いただいている。必要最小限の範囲でフロー情報を収集・蓄積すること、そのフロー情報を C&C サーバ検知以外の用途で使用しないということで、手段の相当性についてもしっかり分析、検討いただいた上でこういった結論を出していただいていた。今後、立法の必要性についても引き続き状況を見ながら検討していきたい。また、フロー情報によって、ネットワークの輻輳などを ISP が日頃から把握することについては、正当業務行為と整理されているものと認識している。
また名和構成員からのご質問で、「適切な事業者団体等への提供」については、電気通信事業法において認定協会として位置づけられている ICT-ISAC への提供を想定してとりまとめていただいた。詳細については、今後、民間ガイドラインを作るところ、総務省もオブザーバーとして参加して検討していく。「営利性」については、情報提供・共有の目的としては想定していない。

廣瀬サイバーセキュリティ統括官室参事官補佐）

若江構成員からのご質問の２点目、第三次とりまとめとの関係については、今回の第四次とりまとめ案で整理いただいたフロー情報の分析は、注意喚起や遮断等ではなく、あくまで「C&C サーバの検知」を目的としたフロー

情報の分析であるというところが異なっている。3点目については、C&C サーバの IP アドレスとポート番号のみであり、タイムスタンプで日時が特定されているようなものではないので、個別の通信要素を明らかにすることにはつながらず、直ちに通信の秘密に該当するとは言えないため共有しても差し支えないと整理されている。

若江構成員）

追加のコメントで、第四次とりまとめ案では、サイバー攻撃のおそれが増大すると、目的の正当性以外の要件である、行為の必要性と手段の相当性が自動的に肯定されるように書かれている。だが、今後のサイバー攻撃のおそれは確実に増大していくと思うので、このような整理では結局すべてのサイバー攻撃対策が正当業務行為になり、適法化されてしまうのではないかと思われる。これは C&C サーバの検知の必要がないから止めるべきと言っているのではなく、このように違法性阻却事由を整理する形でとりまとめを続けていくと、どんどん歯止めがきかなくなっていくような気がするので、ぜひ立法で対応していただきたいという趣旨で発言した。

岡村構成員）

若江構成員がおっしゃった点に関しては、私も手段の相当性が非常に重要だと思う。フロー情報の収集・蓄積が適切に行われているか、目的外利用がないかどうかのチェックについても検討してはどうか。

林構成員）

私自身は、元々アメリカのサイバーセキュリティ情報共有法に似たような法律を作るべきだということを主張しているが、このような法整理のとりまとめの方式であっても、仕組みが作られることは前進と感じている。とはいえ、法律を作らないでガイドラインで対応する以上、現行の法律との関連性の詰めが緩やかになっているのではないかと懸念する。そういう意味では、これが電気通信事業法のどの規定に直接関係するのか、もし仮に法律を変えるとすればどう変えたら良いのかという検討が進むとありがたい。その際に、チェック機能が大事だという岡村構成員のご指摘には同意する。

安達構成員）

C&C サーバの検知に関して、放送業界としても、クリーンなネットワークが必要であると思っているため、これから更なる展開に期待している。

小山構成員）

補足のコメントであるが、名和構成員の先ほどの指摘された情報提供と営利目的の関係について、第四次とりまとめ案の 14 ページで、適切な事業者団体等から提供を受けた ISP がどのように活用するかということまでは議論ができていない。例えば既存の個別のユーザに対する契約に基づくセキュリティサービスなどに展開することで、全体のセキュリティ対策に活用することもあり得るため、サービス料等の設定を制限してしまうと逆にセキュリティ対策に取り組みにくくなる。さきほどの総務省からの回答は、事業者団体等から ISP に対する情報提供を営利目的では行わない、と理解してよいか。

梅村サイバーセキュリティ統括官室参事官）

サイバーセキュリティ対策の目的ということで共有すべきというのが大前提となっているが、ご指摘いただいた通りの認識でよい。

岡村構成員）

サイバー攻撃の情報共有に関して、電気通信事業法第 28 条に事故報告制度があり、中でも特に重大事故については、発生した事故を検証するような場もできている。今後は、サイバーセキュリティという側面から拡張する形でリニューアルすることが求められるので、関係の政令あるいは省令の整備などが必要ないかご検討いただきたい。

藤本構成員）

国民のための情報セキュリティサイトはよく参照、紹介させていただいているので、改修についてぜひよろしくお願いしたい。今、世の中では、DX の取組が進んで、例えばデータの利活用や自動運転等、国民の生活に関連する大きな社会的な変化が起きており、サイバーセキュリティとどういう関連性が出てくるのか等、関心の高いところかと思うので、そういう内容も入れることを検討してほしい。

【資料 34-2　令和 4 年度総務省サイバーセキュリティ関連予算概算要求について】

戸川構成員）

サイバーセキュリティにとって必要な取組を網羅されており評価したい。人材育成を含めて時間がかかる取組かと思うが今後も継続していく必要がある。それから、サイバー攻撃インフラ検知等の積極的セキュリティ対策総合実証、IoT の安全安心かつ適正な利用環境の構築は、総務省のサイバーセキュリティの基盤となる取組だと認識している。特に AI 技術等を積極的に活用するべきだと思うが、国際的な社会情勢が刻々と変化していく中で、冒頭にあった Cybersecurity for ALL の実現に向けて、短期的ではなく長期的な視野を持って、こういった取組を継続していくのは非常に良い。

中尾構成員）

2 ページを見ると、まず「サイバー攻撃インフラ検知等の積極的セキュリティ対策の総合実証」として、サイバー研に関係する①フロー情報分析による C&C サーバ検知技術の実証、②不正な悪性のウェブサイトの検知等を共有など、非常に有効な施策が整理されている。③ネットワークセキュリティ対策技術の導入実証について確認で、ここでの実証は非常に重要であるが、その下の説明で、「ISP におけるセキュリティの対策を強化するため」と書かれている。総務省の事業なので、基本的には ISP のための対策というよりも、国がネットワークの利用者を守るという視点で、ISP がどのような対策を導入して、それの効果がどのくらいあるのかを実証的に検証するという意味かと思うが良いか。

安達構成員）

CYDER について、例えば ICT-ISAC の会員は、無料で受講できるような優遇措置を検討してもよいのではないか。

篠田構成員）

地域セキュリティコミュニティ強化支援事業で 1.2 億円、ナショナルサイバートレーニングセンターの強化で 14 億円の予算が要求されているが、こういった人材育成の仕組みについて、民間と共有され、サイバーカレッジカ

リキュラムにある内容がもっと安く受け取れるようになることを期待している。各自の情熱に依存しているコミュニティの活動は不安定で毎回が奇跡みたいなものであるが、情熱のある人を巻き込み予算が付けば、SECUNITY も動いていくのではないかなと思った。省庁間の役割の違いはあると思うが、IPA の下にあるセキュリティキャンプでも地方を繋ぐ活動はしているので、そういったところと連携できたら良いのではないか。

梅村サイバーセキュリティ統括官室参事官）

中尾構成員から頂いたご質問については、そういった認識である。また、様々なご指摘を頂いたので、室内、関係課とも共有して、必要なことについてしっかり検討していきたい。

【資料 34-3　IoT セキュリティに関連する近年の研究内容の紹介（吉岡構成員)】

鵜飼構成員）

IoT のサイバーセキュリティに関して、研究者というよりはどちらかというと実務者向けで、影響が大きそうな脆弱性情報が BlackHat 等で出てきており、PoC などが出てきてマルウェアに実装されると一気に影響範囲が大きくなる。そういった研究発表のようなものが出たときに、本当に実際の脅威になるのかどうか事前に分析しておく仕組みがあった方が良いのではないか。セキュリティベンダーや ISP の中で独自で行っているところはあると思うが、そういった情報を集約し、脅威分析をして共有すれば、皆が均一な情報にアクセスできて、非常に良いと思う。

岡村構成員）

一般ユーザ保護を目的とするサイバー版 PCR 検査というサービスについては、いわゆる情報弱者がサイバー攻撃のターゲットになっているという傾向が否めないため、大賛成である。

◆議題（4）「東京 2020 オリンピック・パラリンピック大会期間中のサイバー攻撃の動向」について、小山構成員と NICT の井上様より説明。質疑応答、意見交換を実施（非公開)。

（6）閉会

以上